ZENworks 11 SP4 Full Disk Encryption Overview

October 2016

Novell

ZENworks 11 SP4 Full Disk Encryption uses software-based encryption and pre-boot authentication to protect the data on a device's hard disk when the device is powered off or in hibernation mode. The disk encryption and pre-boot authentication settings are applied to the device through a Disk Encryption policy.

1 Disk Encryption

ZENworks Full Disk Encryption supports encryption of both standard hard disks and self-encrypting hard disks.

1.1 Standard Hard Disks

Standard hard disks are any 3.5 or 2.5 inch IDE, PATA, or SATA disks that do not include a hardware encryption chip.

With standard hard disks, ZENworks Full Disk Encryption does sector-based software encryption of the entire disk or selected volumes (partitions). All files on a volume are encrypted, including any temporary files, swap files, or operating system files. Because all files are encrypted, the data cannot be accessed when booting the computer from external media such as a CD-ROM, floppy disk, or USB drive.

You can choose the industry-standard encryption algorithm (AES, Blowfish, DES, or DESX) and key length that best meets your organizations requirements.

NOTE: The cryptographic module used in ZENworks Full Disk Encryption to encrypt standard hard drives is *not* Federal Information Processing Standard (FIPS) 140-2 certified. However, the cryptographic module implements standards consistent with FIPS 140-2 Level 1 certification.

1.2 Self-Encrypting Hard Disks

Self-encrypting hard disks are disks that perform their own encryption via a hardware encryption chip.

ZENworks Full Disk Encryption supports self-encrypting hard disks that are compliant with the *Trusted Computing Group OPAL 2.0* specification. The two modes of support are:

- **Pre-boot authentication with software-based encryption:** This is supported on *ALL* OPAL 2.0 compliant drives.

  Pre-boot authentication is the process of authenticating a user to a device before the device boots to the primary operating system. Using ZENworks pre-boot authentication (ZENworks PBA) in conjunction with Windows login greatly enhances drive security. Software-based encryption adds a second layer of encryption to the drive's native hardware encryption.

  For more information about ZENworks pre-boot authentication, see Section 2, "Pre-Boot Authentication," on page 2.

- **Pre-boot authentication with drive locking:** ZENworks supports drive locking on *SOME* OPAL 2.0 compliant drives. The support is limited because of variations in the way drive manufacturers implement the OPAL 2.0 specification related to drive locking.

  When using this mode, drive locking is initiated during ZENworks PBA initialization. After user authentication occurs through the ZENworks PBA, the drive is unlocked until it is powered off. Only the native hardware encryption is used; ZENworks does not apply software-based encryption in this mode.

  For a list of known drive-locking compatible and incompatible drives, see *ZENworks 11 SP4 Full Disk Encryption Self-Encrypting Drive Support*. For information about how to test a drive for drive-locking compatibility, see *ZENworks 11 SP4 Full Disk Encryption Self-Encrypting Drive Compatibility Testing*.

2 Pre-Boot Authentication

ZENworks Full Disk Encryption protects a device's data when the device is powered off or in hibernation mode. As soon as someone successfully logs in to the Windows operating system, the encrypted volumes are no longer protected and the data can be freely accessed. To provide increased login security, you can use ZENworks Pre-Boot Authentication (ZENworks PBA).

The ZENworks PBA is a Linux-based component. When the Disk Encryption policy is applied to a device with a standard hard disk, a 100 MB partition containing a Linux kernel and the ZENworks PBA is created on the hard disk. When the policy is applied to a device with a self-encrypting hard disk, the Linux kernal and ZENworks PBA are installed to the disk's datastore memory.

During normal operation, the device boots to the Linux partition and loads the ZENworks PBA. As soon as the user provides the appropriate credentials (user ID/password or smart card), the PBA terminates and the Windows operating system boots, providing access to the encrypted data on the previously hidden and inaccessible Windows drives.

The Linux partition is hardened to increase security, and the ZENworks PBA is protected from alteration through the use of MD5 checksums and uses strong encryption for authentication keys.

ZENworks Pre-Boot Authentication is strongly recommended. If you don't use the ZENworks PBA, encrypted data is protected only by Windows authentication.

For more information about ZENworks Pre-Boot Authentication, see the *ZENworks 11 SP4 Full Disk Encryption PBA Reference*

3 Legal Notices

For information about legal notices, trademarks, disclaimers, warranties, export and other use restrictions, U.S. Government rights, patent policy, and FIPS compliance, see https://www.novell.com/company/legal/.

4 Third-Party Materials

All third-party trademarks are the property of their respective owners.